

POLÍTICA DE KYC

“CONHEÇA SEU CLIENTE”

DALPAY

DAL SOLUÇÕES DE PAGAMENTOS LTDA

Data: 21 de junho de 2024.

Versão 1.0

APRESENTAÇÃO

Esta **Política de KYC (“Conheça Seu Cliente”)** está dentro do escopo do Programa e Práticas de PLD/CFT aplicadas aos serviços oferecidos pela **DAL SOLUÇÕES DE PAGAMENTOS LTDA**, pessoa jurídica de direito privado, inscrita no CNPJ n.º 55.196.715/0001-53, com sede na Rua Visconde de Pirajá, n.º 414, Sala 718, Ipanema, Rio de Janeiro – RJ, CEP: 22.410-905, doravante denominada simplesmente **“DALPAY”**.

Esta Política, junto ao Código de Ética e Conduta, faz parte do Programa de Compliance da **DALPAY**, o qual visa nortear e demonstrar o controle do comportamento organizacional da **DALPAY** e alinhamentos de conformidade, por meio de um complexo de controles internos e procedimentos, os quais consagram os pilares das narrativas de Governança Corporativa: transparência, equidade, prestação de contas e responsabilidade corporativa.

A **DALPAY** se compromete a desenvolver um conjunto de controles internos no intuito de assegurar: **(i)** o correto cumprimento da legislação; **(ii)** a utilização eficiente e eficaz de todos os recursos; **(iii)** a redução dos níveis de incerteza e minimização da ocorrência de riscos financeiros, operacionais, regulatórios, de imagem ou legais.

Esta política também é parte integrante da Política de Privacidade, documento que orienta e estabelece as diretrizes corporativas de colaboradores envolvidos na operação para a proteção dos ativos de informação e a prevenção de eventual responsabilidade legal.

A **DALPAY**, em atendimento a legislação vigente e em defesa de seus próprios interesses comerciais, determina aos seus colaboradores e parceiros a não divulgação de dados inerentes ao ambiente de trabalho e de seus clientes. Os colaboradores da **DALPAY** são diretamente responsáveis pelo devido armazenamento e manipulação dos documentos enviados, devendo garantir o sigilo e a confidencialidade dos dados garantindo a exposição a terceiros ou outros colaboradores da empresa que não tenham alçada de acesso a essas informações.

A **DALPAY** também atua em observância a Lei do Marco Civil na Internet Lei n.º

12.965/2014, bem como a Lei nº 13.709/2018 (LGPD - Lei Geral de Proteção de Dados) e tem como premissa a manutenção do sigilo e segurança das informações de seus clientes.

A presente Política visa a promover a adequação das atividades operacionais da Empresa com as normas pertinentes aos crimes de lavagem de dinheiro e financiamento do terrorismo (“LD/FT”).

Todos os estagiários, funcionários, prestadores de serviços, exchanges e sócios devem adotar as melhores práticas no cadastramento de clientes e dedicar especial atenção aos conceitos e atividades que auxiliam na prevenção e combate à LD/FT. As leis e regulamentos atrelados a este delito, bem como as regras desta Política devem ser obrigatoriamente cumpridas.

A Política identificará o conceito de lavagem de dinheiro, as etapas que configuram o delito e as características de pessoas e produtos suscetíveis a envolvimento com este crime.

Além disso, serão tipificadas as operações de lavagem de dinheiro, identificados os controles utilizados pela **DALPAY** e definidas as regras para aplicação dos formulários de “KYC” ou “Conheça seu Cliente”.

O conhecimento de algum indício de lavagem de dinheiro deverá ser comunicado ao departamento de Controles Internos e Compliance (“Compliance”), sendo este responsável por averiguar as informações reportadas e, caso aplicável, comunicar aos órgãos reguladores.

O Compliance será igualmente responsável por disponibilizar aos colaboradores da **DALPAY** treinamentos e palestras que promovam a conscientização sobre o crime de lavagem de dinheiro e desenvolver campanhas/atividades que auxiliem na detecção de operações que caracterizem indícios deste crime.

Esta Política, junto ao Código de Ética e Conduta, faz parte do Programa de Compliance da **DALPAY**, o qual visa nortear e demonstrar o controle do

comportamento organizacional da **DALPAY** e alinhamentos de conformidade, por meio de um complexo de controles internos e procedimentos, os quais consagram os pilares das narrativas de Governança Corporativa: transparência, equidade, prestação de contas e responsabilidade corporativa.

Os colaboradores da **DALPAY** são diretamente responsáveis pelo devido armazenamento e manipulação dos documentos enviados, devendo garantir o sigilo e a confidencialidade dos dados garantindo a exposição a terceiros ou outros colaboradores da empresa que não tenham alçada de acesso a essas informações.

A **DALPAY** também atua em observância a lei do Marco Civil na Internet Lei nº 12.965/2014, bem como a Lei nº 13.709/2018 (LGPD - Lei Geral de Proteção de Dados) e tem como premissa a manutenção do sigilo e segurança das informações de seus clientes, bem como com a Lei Nº 14.478, DE 21 DE DEZEMBRO DE 2022 que dispõe sobre diretrizes a serem observadas na prestação de serviços de ativos virtuais e na regulamentação das prestadoras de serviços de ativos virtuais, bem como observando o Decreto nº 11.563 de 2023 que fixou a competência do Banco Central do Brasil como órgão regulador do mercado de criptoativos.

A **DALPAY** observa as seguintes diretrizes, conforme a Lei 14.478/2022:

- I - Livre iniciativa e livre concorrência;
- II - boas práticas de governança, transparência nas operações e abordagem baseada em riscos;
- III - segurança da informação e proteção de dados pessoais;
- IV - proteção e defesa de consumidores e usuários;
- V - Proteção à poupança popular;
- VI - solidez e eficiência das operações; e
- VII - prevenção à lavagem de dinheiro e ao financiamento do terrorismo e da proliferação de armas de destruição em massa, em alinhamento com os padrões internacionais.

A expressão “lavagem de dinheiro” consiste na realização de operações comerciais ou financeiras com a finalidade de incorporar recursos, bens e serviços obtidos

ilicitamente.

Etapas do crime e lavagem de dinheiro:

O processo de lavagem de dinheiro envolve 03 (três) etapas, são elas:

1) Colocação: é a etapa em que o criminoso introduz o dinheiro obtido ilicitamente no sistema econômico mediante depósitos, compra de instrumentos negociáveis ou compra de bens. Trata da remoção do dinheiro do local que foi ilegalmente adquirido e sua inclusão, por exemplo, ao mercado financeiro;

2) Ocultação: é o momento que o agente realiza transações suspeitas e caracterizadoras do crime de lavagem. Nesta fase, diversas transações complexas se configuram para desassociar a fonte ilegal do dinheiro;

3) Integração: nessa etapa, o recurso ilegal integra definitivamente o sistema econômico e financeiro. A partir deste momento, o dinheiro recebe aparência lícita.

A **DALPAY** reforça seu compromisso com a conformidade legal, ética e a prevenção de práticas ilícitas, assegurando transparência, segurança e integridade em suas operações relacionadas a blockchain, criptomoedas e tecnologia financeira.

Conheça seu Cliente (KYC) é um procedimento legal obrigatório pelo qual as instituições financeiras, incluindo bancos, corretoras de criptomoedas e outros provedores de serviços financeiros, coletam dados de identificação e informações de contato dos usuários existentes e potenciais. O seu objetivo principal é prevenir fraudes, lavagem de dinheiro, financiamento do terrorismo e outras atividades ilícitas e garantir a devida diligência do usuário como parte dos esforços de conformidade para a Prevenção à Lavagem de Dinheiro e para o Combate ao Financiamento do Terrorismo (PLD/CFT).

A principal função do KYC (Know Your Customer) no setor de ativos digitais é identificar indivíduos potencialmente mal-intencionados, impedindo seu acesso ao

ecossistema e prevenindo atividades como lavagem de dinheiro, financiamento do terrorismo e outras formas de fraude. Isso contribui para criar um ambiente mais seguro para todos os participantes. Um programa KYC abrangente permite que empresas de criptomoedas conheçam seus clientes e avaliem com precisão o risco que representam para suas plataformas e para a comunidade em geral.

O papel do KYC no setor de criptomoedas é semelhante ao das instituições financeiras tradicionais, visando proteger os negócios, os clientes e a comunidade ao evitar o acesso de indivíduos mal-intencionados.

Um processo de integração KYC robusto permite que os provedores de serviços de ativos digitais eliminem o anonimato, obtenham informações importantes do usuário, realizem uma verificação de identidade eficiente e conduzam uma análise de risco que resulta na decisão final de aprovar ou recusar a solicitação de abertura de conta do potencial usuário.

Os usuários comprometem-se a não utilizar os serviços da **DALPAY** para facilitar ou participar de atividades de lavagem de dinheiro ou financiamento do terrorismo, e concordam em relatar imediatamente qualquer atividade suspeita à **DALPAY**.

A **DALPAY** reserva-se o direito de atualizar e revisar regularmente suas políticas e procedimentos de KYC para garantir a conformidade contínua com as leis e regulamentos aplicáveis.

Os usuários reconhecem e concordam que a **DALPAY** poderá divulgar informações relevantes sobre atividades suspeitas de lavagem de dinheiro ou financiamento do terrorismo às autoridades competentes, conforme exigido por lei.

Os usuários reconhecem e concordam que a **DALPAY** poderá, a seu critério exclusivo, congelar ou reter quaisquer fundos suspeitos de serem relacionados à lavagem de dinheiro ou ao financiamento do terrorismo, até que a investigação adequada seja concluída.

ÍNDICE

1. TERMOS E DEFINIÇÕES.....	8
2. OBJETIVO	10
3. RESPONSABILIDADES.....	13
4. COMO SE DÁ O KYC?	19
5. PROCEDIMENTOS INTERNOS ADOTADOS PELA EMPRESA.....	27
6. GERENCIAMENTO DE RISCO	29
7. CRITÉRIOS DE APROVAÇÃO	34
8. LIMITES OPERACIONAIS.....	36
9. ABORDAGEM BASEADA EM RISCO	40
10. MECANISMOS E MÉTRICAS DE AVALIAÇÃO DE RISCO.....	45
11. PESSOAS EXPOSTAS POLITICAMENTE (PEP)	47
12. PROTEÇÃO DE DADOS PESSOAIS.....	47
13. DIRETORIA DE ÉTICA E COMPLIANCE	48
14. DEPARTAMENTO DE COMPLIANCE.....	48
15. ATUALIZAÇÃO CADASTRAL.....	50
16. CANAL DE DENÚNCIAS.....	50
17. LEGISLAÇÃO APLICÁVEL E FORO	51
18. APROVAÇÃO E VIGÊNCIA.....	51

1. TERMOS E DEFINIÇÕES

1.1. Os conceitos e siglas abaixo referem-se aos termos presentes ao longo desta Política:

TERMO	DEFINIÇÃO
“ANBIMA”	Associação Brasileira das Entidades dos Mercados Financeiros e de Capitais.
“BACEN”	Banco Central do Brasil e órgão regulador do mercado conforme Decreto nº 11.563/2023.
“Over The Counter (OTC)”	Mercado de balcão, onde há negociar direta de ativos.
“Exchange de Criptoativos”	Empresa que possui uma plataforma onde compradores e vendedores podem ofertar criptoativo em um livro de ofertas aberto.
“CEIS”	Cadastro de Empresas Inidôneas e Suspensas.
“Cadastro”	repositório de dados e documentos fornecidos pelos clientes e validados pelo Compliance da DALPAY .
“CEPIM”	Cadastro de Entidades Privadas Sem Fins Lucrativos Impedidas.
“Cliente/Usuário”	Pessoa física ou jurídica, que utiliza os Serviços oferecidos pela DALPAY .
“CNEP”	Cadastro Nacional de Empresas Punidas.
“Conselho de Controle de Atividades Financeiras (COAF)”	Órgão (Unidade de Inteligência Financeira Brasileira) responsável pela aplicação de sanções administrativas, a partir do recebimento, exame e identificação de ocorrências suspeitas de atividades ilícitas de lavagem de dinheiro e financiamento do terrorismo, além de proceder com a comunicação as autoridades competentes para a instauração dos procedimentos cabíveis, quando da conclusão pela existência de fundados indícios de crimes de lavagem de dinheiro e financiamento ao terrorismo;

“Criptoativos”	Ativos digitais criptografados, podendo ser criptomoedas ou tokens (Ex.: Bitcoin, Ethereum, Lite Coin);
“Lavagem de Dinheiro”	Consiste na realização de operações comerciais ou financeiras com a finalidade de incorporar recursos, bens e Serviços obtidos ilícitamente;
“FBI”	Federal Bureau of Investigation.
“FEBRABAN”	Federação Brasileira de Bancos.
“GAFI/FATF”	Grupo de Ação Financeira contra Lavagem de Dinheiro e Financiamento ao Terrorismo (organização intergovernamental).
“INTERPOL”	International Criminal Police Organization.
“Know Your Customer (KYC)”	Procedimento de “Conheça seu Cliente” que visa identificar, verificar, validar e qualificar os clientes, de modo que seja possível apreciar, avaliar e classificar o cliente com a finalidade de conhecer o seu perfil de risco e sua capacidade econômico-financeira.
“Know Your Partner (KYP)”	Procedimento de due diligence para parceiros.
“Know Your Employee (KYE)”	Procedimento de due diligence na admissão e contratação de colaboradores.
“Know Your Transactions (KYT)”	Procedimento de due diligence para identificar, monitorar e relatar transações que possam estar associadas a atividades criminosas, incluindo a lavagem de dinheiro e o financiamento do terrorismo;
“OFAC”	Office of Foreign Assets Control.
“Pessoa Exposta Politicamente (PEP)”	Conforme a Circular do Bacen nº 3.978/20, consideram-se PEP os agentes públicos que desempenham ou tenham desempenhado, nos últimos 05 (cinco) anos, no Brasil ou em países, territórios e dependências estrangeiras, cargos, empregos ou funções públicas relevantes, assim como seus representantes, familiares e outras pessoas de seu relacionamento próximo.

“UNSC”

United Nations Security Council.

2. OBJETIVO

2.1. O objetivo central do Compliance é capacitar os colaboradores, prestadores de serviços, parceiros e administradores, através de treinamentos, disponibilização de conteúdo e determinação de diretrizes relativas a assuntos relacionados à conformidade legal dos negócios **DALPAY**, acompanhando e revisando os relatórios do departamento quanto a eventuais descumprimentos regulamentares e legais.

2.2. Além do monitoramento das operações é realizado o processo de Due Dilligence na avaliação de clientes, parceiros, prestadores de serviços e negócios em processo de aquisição, como processo complementar na validação dos dados cadastrais fornecidos.

2.3. O Procedimento KYC tem como escopo principal proteger a **DALPAY** do envolvimento com atividades ilícitas, bem como indivíduos, jurisdições ou entidades sancionadas, além de garantir que a **DALPAY** cumpra integralmente todas as respectivas leis, regulamentos ou normas pertinentes ao escopo de PLD/CFT.

2.4. O procedimento visa, precipuamente, identificar os reais detentores dos ativos e recursos que circulam na **DALPAY**, sendo o elemento mais importante no processo de prevenção à lavagem de dinheiro e ao financiamento do terrorismo, visando prover direcionamento e padronização para o início, a manutenção e o monitoramento do relacionamento com aqueles que utilizam ou pretendam utilizar os produtos e serviços da **DALPAY**.

2.5. No procedimento se consigna a estratégia de verificação prévia, em que todos os clientes que desejam transacionar com a **DALPAY** têm suas informações meticulosamente analisadas, como forma de evitar a realização de negócios com agentes suspeitos ou potencialmente criminosos. Assim sendo, a **DALPAY** se resguarda no direito de recusar a realizar transações com clientes cujos registros e fichas criminais contenham marcações ou apontamentos de ocorrências ou fatos

negativos e desabonadores.

2.6. Além disso, a **DALPAY** realiza ainda a chamada “Avaliação Baseada em Riscos”, criada para mitigar os riscos de lavagem de dinheiro e financiamento ao terrorismo. A **DALPAY** utiliza direcionadores de risco e distribuí um determinado peso, de modo a atribuir a cada cliente e operação o grau de suscetibilidade à lavagem de dinheiro e ilícitos financeiros, equacionando com suas métricas de apetite de risco. A partir do risco associado ao cliente, a **DALPAY** aprova o início e o prosseguimento do relacionamento. Neste documento estão definidos, também, os papéis e responsabilidades no que tange à decisão das medidas a serem empregadas.

2.7. A **DALPAY** opera como prestadora de serviços de tecnologia financeira, especializada em ativos digitais, oferecendo uma ampla gama de soluções aos seus Clientes por meio de sua Plataforma, bem como serviços de integrações com instituições financeiras e varejistas, oferecendo funcionalidades para facilitar e dar segurança às transações realizadas por você na Plataforma da **DALPAY**. As transações são realizadas diretamente entre os Usuários na própria Plataforma, sem qualquer interferência ou influência da **DALPAY**, de forma que toda a negociação, comunicação e efetivação da operação é realizada sem a participação da **DALPAY**.

2.8. As diretrizes e procedimentos desta Política foram criados conforme a Circular do Banco Central do Brasil nº 3.681/2013 e Resolução do Banco Central do Brasil nº 25/2020, e suas respectivas alterações. A presente Política foi elaborada de forma compatível com o porte, a natureza, a complexidade, a estrutura e o modelo de negócio da **DALPAY**.

2.9. A presente Política estabelece as diretrizes e padrões de controles e monitoramento que garantam a conformidade, funcionamento e visam mitigar os riscos da **DALPAY**.

2.10. As regras aqui definidas devem ser atualizadas pela Área de Compliance da **DALPAY**, através da análise de eventuais atualizações, revogações ou publicações de novas normas aplicáveis, bem como devem ser revisadas pela diretoria de acordo com periodicidade prevista na regulamentação em vigor.

2.11. Esta Política dispõe sobre as diretrizes referentes ao gerenciamento de risco de crédito, de liquidez e operacional, visando a conformidade da **DALPAY** com as regulamentações e legislações vigentes, a proteção dos negócios e situação econômico-financeira da **DALPAY**.

2.12. Analisamos as leis e regulamentos específicos e construímos nosso programa de conformidade dentro dessas jurisdições para atender a esses requisitos, além de seguir os padrões internacionais relevantes. A legislação relacionada à Prevenção à Lavagem de Dinheiro (PLD) e ao Combate ao Financiamento do Terrorismo (CTF), juntamente com a orientação da unidade local de inteligência financeira, são os pilares da nossa abordagem KYC.

2.13. O desenvolvimento das medidas KYC na **DALPAY** é um processo colaborativo que envolve membros sêniores da equipe KYC, especialistas do setor Jurídico, Tecnologia e Operações, além de membros sêniores da equipe de gerenciamento. Os principais componentes de nossa estrutura KYC incluem verificação de identidade (comparação biométrica com documentos de identidade emitidos pelo governo, análise da autenticidade desses documentos, verificações de prova de vida e utilização de tecnologias de Reconhecimento Óptico de Caracteres - OCR - para validar informações fornecidas pelo usuário), geolocalização de IP, due diligence aprimorada e triagem em relação a sanções, Pessoas Politicamente Expostas (PPE), bancos de dados de mídia negativa, listas de crimes financeiros e aplicação regulatória.

2.14. A equipe de Conformidade da **DALPAY** está empenhada em manter um programa KYC que cumpra todos os requisitos legais e regulatórios, proporcionando uma experiência consistente aos nossos usuários. Uma forma de alcançar isso é avaliar continuamente tecnologias inovadoras e possíveis parcerias com fornecedores que possam ajudar a reduzir o atrito associado aos procedimentos KYC.

3. RESPONSABILIDADES

3.1. É responsabilidade da **DALPAY** manter políticas, procedimentos e controles adequados para mitigar e tratar os riscos de compliance e riscos legais, especialmente no que diz respeito à prevenção à lavagem de dinheiro (“PLD”) e ao combate ao financiamento do terrorismo (“FT”).

3.2. A **DALPAY** destaca que possui a responsabilidade de combater a entrada de capital originário de atividades ilícitas, espúrias e criminosas, adotando as diligências necessárias para a prevenção de crimes financeiros e condutas contrárias aos valores de probidade que são parte integrante de sua filosofia de negócio. Portanto, para a aplicação das diretrizes da presente política, o Programa de Compliance da **DALPAY** inclui:

- a) Sistema de controles internos para verificar e estabelecer a conformidade de cada área da **DALPAY**;
- b) Treinamento da Administração e seus colaboradores para alinhamento com uma cultura íntegra de conformidade com as regras, boas práticas, valores éticos e procedimentos de Compliance;
- c) Estruturação de Departamento de Compliance;
- d) Existência de políticas e procedimentos claros;
- e) Procedimentos de Client Due Diligence, realizados no âmbito do programa de Know Your Customer (KYC);
- f) Due Diligence de Terceiros para compreensão dos riscos inerentes ao relacionamento (riscos à imagem, de suborno e corrupção) através de programas de Know Your Partner (KYP) e KnowYour Employee (KYE).

3.3. A **DALPAY** opera com ferramentas de monitoramento (operações e cadastro), classificação de risco, alertas, análise e comunicação ao COAF, para detecção de

operações e situações suspeitas de PLD/FT. Utiliza ferramentas para a execução de análise de Due Diligence, utilizando bases reputacionais como listas de sanções nacionais, PEP, listas restritivas internacionais, entre outras.

3.4. O monitoramento tem início com a coleta de documentos do cliente, que seguem as indicações dos artigos 16 e 18 da Circular nº 3.978 de 2020 do BACEN, que dispõe:

“Art. 16. As instituições referidas no art. 1º devem adotar procedimentos de identificação que permitam verificar e validar a identidade do cliente

§ 1º Os procedimentos referidos no caput devem incluir a obtenção, a verificação e a validação da autenticidade de informações de identificação do cliente, inclusive, se necessário, mediante confrontação dessas informações com as disponíveis em bancos de dados de caráter público e privado.

§ 2º No processo de identificação do cliente devem ser coletados, no mínimo:

I - O nome completo e o número de registro no Cadastro de Pessoas Físicas (CPF), no caso de pessoa natural; e

II - a firma ou denominação social e o número de registro no Cadastro Nacional da Pessoa Jurídica (CNPJ), no caso de pessoa jurídica.

§ 3º No caso de cliente pessoa natural residente no exterior desobrigada de inscrição no CPF, na forma definida pela Secretaria da Receita Federal do Brasil, admite-se a utilização de documento de viagem na forma da Lei, devendo ser coletados, no mínimo, o país emissor, o número e o tipo do documento.

§ 4º No caso de cliente pessoa jurídica com domicílio ou sede no exterior desobrigada de inscrição no CNPJ, na forma definida pela Secretaria da Receita Federal do Brasil, as instituições devem coletar, no mínimo, o nome da empresa, o endereço da sede e o número de identificação ou de registro da empresa no respectivo país de origem.

Art. 18. As instituições mencionadas no art. 1º devem adotar procedimentos

que permitam qualificarseus clientes por meio da coleta, verificação e validação de informações, compatíveis com o perfil de risco do cliente e com a natureza da relação de negócio

§ 1º Os procedimentos de qualificação referidos no caput devem incluir a coleta de informações que permitam:

- I - Identificar o local de residência, no caso de pessoa natural;
- II - identificar o local da sede ou filial, no caso de pessoa jurídica; e
- III - avaliar a capacidade financeira do cliente, incluindo a renda, no caso de pessoanatural, ou o faturamento, no caso de pessoa jurídica.

§ 2º A necessidade de verificação e de validação das informações referidas no §1º deve ser avaliada pelas instituições de acordo com o perfil de risco do cliente e com a natureza da relação de negócio.

§ 3º Nos procedimentos de que trata o caput, devem ser coletadas informações adicionais do cliente compatíveis com o risco de utilização de produtos e serviços na prática da lavagem de dinheiro e do financiamento do terrorismo.

§ 4º A qualificação do cliente deve ser reavaliada de forma permanente, de acordo com a evolução da relação de negócio e do perfil de risco.

§ 5º As informações coletadas na qualificação do cliente devem ser mantidas atualizadas.

§ 6º O Banco Central do Brasil poderá divulgar rol de informações a serem coletadas, verificadase validadas em procedimentos específicos de qualificação de clientes.”

3.5. A **DALPAY** não realiza parcerias nem possui relações com países ou clientes presentes em listas de sanções nacionais e internacionais;

3.6. É responsável pelo Programa de Prevenção à Lavagem de Dinheiro e ao Financiamento do Terrorismo (PLD/FT) o Diretor da **DALPAY**, Sr. **DAVIDSON DE ALENCAT LEITE**, o qual deverá cumprir e fazer cumprir as regras e procedimentos

estabelecidos.

3.7. A responsabilidade pela elaboração e redação da presente política é da Dra. Jessyca Arieira, OAB/RJ 201.582, contratada pela **DALPAY**. Esta política deve ser revisada sempre que necessário ou, no mínimo, anualmente.

3.8. Todos os Colaboradores da **DALPAY** que desempenham quaisquer atividades correlatas aos riscos dispostos nesta Política tem o dever de zelar pela conformidade dos processos de gerenciamento de riscos.

3.9. Cabe aos Administradores/Alta Administração da **DALPAY**:

a) Fazer constar em relatório anual de gerenciamento de riscos de liquidez sua responsabilidade pelas informações divulgadas;

b) Assegurar o cumprimento desta Política;

c) Revisar e aprovar, anualmente ou na menor periodicidade exigida pela regulamentação, esta Política de Gerenciamento de Riscos;

d) Aprovar todos os procedimentos a serem definidos referentes ao disposto nesta Política, como a matriz de riscos, matriz de classificação de Clientes, limites de tolerância ao risco, tratamento de riscos, plano de continuidade de negócios da **DALPAY**, entre outros;

e) Nomear o Diretor de Riscos, que terá as atividades da gestão de risco separadas das atividades da área de auditoria interna da **DALPAY**.

3.10. Cabe ao Diretor de Riscos (CRO) da **DALPAY**:

a) Definir objetivos e elaborar, em conjunto com a Área de Compliance, políticas e procedimentos relacionados ao planejamento estratégicos de risco, matriz de riscos, limites de tolerância ao risco, plano de respostas aos riscos e plano de continuidade de negócios;

b) Monitorar o grau de aderência dos processos da estrutura de gerenciamento de riscos às políticas;

c) Informar periodicamente à Alta Administração sobre as políticas, procedimentos e eventos objetos desta Política, bem como eventuais atualizações;

d) Assegurar o cumprimento desta Política, pelos gestores com funções ou atividades de negócios que geram exposição a riscos, e pelos responsáveis pela definição dos métodos para identificação, avaliação e monitoramento do grau de exposição a riscos operacionais.

3.11. Cabe a área de Compliance, Riscos e Controles Internos:

a) Elaborar todos os procedimentos a serem definidos referentes ao disposto nesta Política, como a matriz de riscos, limites de tolerância ao risco, tratamento de riscos, plano de continuidade de negócios da **DALPAY**, entre outros;

b) Monitorar a aderência das áreas e processos da **DALPAY** a esta Política; o Assegurar o cumprimento desta Política

I – OPERAÇÕES REALIZADAS ATRAVÉS DAS CORRETORAS EXTERNAS

3.12. Para operações realizadas através da Plataforma de corretoras externas, como a **BINANCE**, a responsabilidade pela verificação de KYC (Conheça Seu Cliente) é exclusiva da corretora. A **DALPAY** confia integralmente no processo de cadastro e verificação conduzido pelas corretoras, que são responsáveis por fornecer o ambiente de negociação, cadastro e verificação dos usuários dentro de sua plataforma. A **DALPAY** não possui controle, gerência ou acesso a este processo, não se responsabilizando pela veracidade dos dados fornecidos ou pelo tratamento desses dados. Qualquer disputa, erro ou fraude relacionada ao processo de cadastro deve ser resolvida diretamente com a corretora escolhida.

3.12.1. Todas as questões relacionadas ao cadastro, veracidade dos dados, tratamento de informações e segurança dos dados fornecidos são de inteira responsabilidade da corretora externa. Qualquer disputa, erro ou fraude relacionada ao processo de cadastro deve ser resolvida diretamente com a respectiva corretora.

3.12.2. De igual maneira, a **DALPAY** não terá qualquer responsabilidade por eventual mau uso por parte do Usuário ou de terceiros, por falhas de segurança na Plataforma/Site da corretora, nem por eventuais ataques sofridos pelo Usuário.

3.13. Para assegurar a segurança das transações e prevenir fraudes, a **DALPAY** realiza uma verificação adicional do CPF ou CNPJ dos Usuários cadastrados em sua Plataforma, através de fornecedores homologados. Essa verificação é realizada pelas seguintes empresas:

- **COMBATEAFRAUDE S.A.** – CNPJ n.º 34.102.645/0001-57, com sede na Rua Tiradentes, n.º 1077, 5º Andar, Centro, Venâncio Aires – RS, CEP: 95.800-000, site: www.caf.io/pt ;
- **NETRIN CONSULTORIA E SERVIÇOS EM TECNOLOGIA DA INFORMAÇÃO LTDA.** – CNPJ n.º 13.384.727/0001-61, com sede na Av. Theodomiro Porto da Fonseca, n.º 3101, Edifício 08, Sala E, Duque de Caxias, São Leopoldo – RS, CEP: 93.020-080, site: www.netrin.com.br .

3.14. Essa verificação adicional é realizada por mera liberalidade da **DALPAY** e como uma proteção extra sendo adotada exclusivamente para aumentar a segurança das transações realizadas sob nossa intermediação, mas não altera a responsabilidade da corretora externa pelo processo de cadastro e verificação de seus próprios usuários.

II – OPERAÇÕES REALIZADAS NA PLATAFORMA DALPAY

3.15. Para operações realizadas dentro de nossa Plataforma, a **DALPAY** realiza uma verificação de KYC (Conheça Seu Cliente) mais completa, específica para Usuários da Plataforma. Nesses casos, o monitoramento do cadastro de clientes é atualizado a cada 90 (noventa) dias, incluindo a obtenção de novas certidões e a atualização da lista de sanções internacionais e nacionais, validadas para garantir o monitoramento e a auditoria dos entes públicos nas transações realizadas pelos Usuários. Além disso, os Usuários são aprovados após a verificação da compatibilidade financeira, extraída de dados públicos da Receita Federal do Brasil.

3.16. Entretanto, é importante ressaltar que a **DALPAY** disponibiliza sua tecnologia para que outros Comerciantes operem tanto em sua Plataforma quanto em plataformas de corretoras externas. Nesses casos, os Comerciantes estão na linha de frente das transações e assumem integralmente os riscos dos recebimentos em suas contas bancárias. Assim, a **DALPAY** não se expõe diretamente como responsável pela verificação de KYC nessas operações, cabendo aos Comerciantes a responsabilidade de garantir a robustez de seus próprios processos de verificação.

4. COMO SE DÁ O KYC?

4.1. O processo de “onboarding” se inicia no cadastro do Cliente, tratando-se de um elemento essencial na prevenção e combate ao crime de lavagem de dinheiro e financiamento ao terrorismo. O cumprimento rigoroso da política de regras e procedimentos do departamento de cadastro é imperativo para assegurar a integridade e conformidade das operações da **DALPAY**.

4.2. O Usuário deverá se cadastrar em nossa Plataforma/Site, onde deverá informar um e-mail para receber um link de autenticação, além de seu nome completo e CPF. Adicionalmente, será necessário preencher um formulário com as seguintes informações:

- a) **PESSOA FÍSICA:** i) nome e sobrenome; ii) Cadastro de Pessoa Física (CPF); iii) endereço completo; iv) data de nascimento; v) indicação do montante semanal ou mensal pretendido;

b) PESSOA JURÍDICA: i) nome empresarial; ii) Cadastro Nacional de Pessoa Jurídica (CNPJ); iii) endereço institucional; iv) nome e sobrenome do sócio/representante responsável pelo cadastro; v) Cadastro de Pessoa Física (CPF) do sócio/representante responsável pelo cadastro; vi) Indicação do montante semanal ou mensal pretendido.

4.3. O respectivo formulário é disponibilizado aos clientes no ato do cadastramento dos dados, ou seja, antes do início de suas operações. O preenchimento do formulário poderá ser solicitado pelo Compliance quando este entender necessário o preenchimento e/ou atualização dos respectivos dados.

4.4. A ficha cadastral da **DALPAY** é clara, objetiva e segregada para pessoas físicas e jurídicas. A análise cuidadosa de toda a documentação é realizada para confirmar a veracidade do cadastro.

4.5. Considerando as principais diretrizes e regras existentes no mercado financeiro e de negociação de criptoativos, bem como a análise dos principais casos de lavagem de dinheiro, é possível relacionar as pessoas mais sensíveis de envolvimento com o crime de lavagem de dinheiro.

4.6. Os formulários de “Conheça seu cliente” (“KYC”) devem ser aplicados aos clientes pessoas físicas e jurídicas. Todos os campos devem ser preenchidos com seriedade e clareza, permitindo a exata definição do perfil do cliente.

4.7. O formulário “Conheça seu cliente” (KYC) será arquivado eletronicamente, quando assim preenchido, ou fisicamente junto ao dossiê cadastral do cliente.

4.8. A **DALPAY** supervisiona constantemente as condutas profissionais e pessoais de seus colaboradores, reprimindo severamente qualquer descumprimento dos princípios éticos da instituição.

4.9. Conforme a indicação do montante pretendido e limites de transação estabelecidos pela **DALPAY**, recebemos a documentação do Usuário ou parceiro como 1ª (primeira) etapa do processo de onboarding:

1ª ETAPA – ENVIO DE DOCUMENTOS

4.10. O candidato a Cliente envia a documentação exigida, sendo:

a) PESSOA FÍSICA:

- Documento de identidade com emissão no máximo de 10 (dez) anos (RG, CNH, Passaporte ou RNE);
- Telefone celular;
- Uma imagem frente e verso do documento de identidade (RG ou CNH) com foto;
- Uma selfie segurando o mesmo documento de identificação;
- Comprovante de residência com data máxima de 03 (três) meses anteriores;
- Comprovante de renda (declaração de IRPF, contracheque, extrato bancário e etc);
- Informações profissionais: informações sobre emprego atual, fonte de renda e atividade econômica;
- Origem dos Fundos: documentação que comprove a origem dos recursos a serem movimentados na relação de negócio (atividade empresarial, atividade profissional, herança, venda de bens, indenização, jogos de loteria, donativos/caridade ou outros);
- Opção de destino dos fundos (ex: transações diárias, poupança, constituição de depósito a prazo, transferência internacional, reembolso de empréstimo, investimento, etc);
- Recibo da declaração da Instrução Normativa n.º 1888/2019 dos últimos 03 meses;
- Endereço de wallet;
- Outras informações que a **DALPAY** possa exigir e sejam necessárias para

essa finalidade;

b) PESSOA JURÍDICA: O cadastro de pessoas jurídicas deverá ser realizado por um representante legal devidamente autorizado pela sociedade, apresentando os documentos necessários à comprovação da representação legal da sociedade, como:

- Documento de Identificação dos Sócios e Administradores: Uma imagem frente e verso do documento de identidade (RG ou CNH com CPF) com foto;
- Selfie dos Sócios e Administradores: Uma selfie segurando o mesmo documento de identificação;
- Comprovante de residência dos Sócios e Administradores: Contas de serviço público (água, luz, telefone, etc) com data máxima de 03 (três) meses anteriores;
- CNPJ;
- Contrato Social ou Estatuto Social de Constituição da Empresa e demais alterações (se houver);
- Comprovante de endereço institucional com data máxima de 03 (três) meses anteriores;
- Balanço ou declaração de faturamento assinado pelo contador e pelos respectivos sócios;
- Declaração IRPJ;
- Registro de Atividade Econômica (licenças, alvarás, etc);
- Recibo da declaração da Instrução Normativa n.º 1888/2019 dos últimos 03 meses;
- Comprovante de Renda dos Sócios;
- Volume mensal desejado;
- Opção de destino dos fundos (ex: transações diárias, poupança,

constituição de depósito a prazo, transferência internacional, reembolso de empréstimo, investimento, etc);

- Endereço da Wallet: endereço da wallet de titularidade da empresa e informações da rede;
- Outras informações que a **DALPAY** possa exigir e sejam necessárias para essa finalidade.

4.11. Após o envio dos documentos e preenchimento do formulário pelo candidato a Cliente, a documentação é encaminhada ao Diretor da **DALPAY**, Sr. **DAVIDSON DE ALENCAR LEITE**, para verificação e elaboração da 2ª etapa.

4.12. Após o envio dos documentos a equipe interna verifica a veracidade dos documentos apresentados para garantir que pertençam ao Cliente que efetuou o envio, e se de fato constam com as informações na base de dados da Receita Federal do Brasil, Banco Central do Brasil e Sistema Público do Brasil, verificando, ainda, se o Usuário se encontra em jurisdição proibida.

4.13. Após a conclusão da verificação para garantir a autenticidade e veracidade dos documentos conforme descrito acima, será iniciada a 2ª (segunda) etapa do processo de onboarding.

2ª ETAPA – VERIFICAÇÃO FINANCEIRA E JURÍDICA NO SISTEMA INTERNO

4.14. Na 2ª etapa, o sistema revisita as informações elencadas para verificar se há algum impedimento jurídico, financeiro ou alguma atividade atípica em nome do Usuário.

4.15. Verificam-se as seguintes informações financeiras e jurídicas do Cliente:

- a) Renda Mensal estimada e declarada (em R\$);
- b) Patrimônio estimado e declarado;
- c) Análise do endereço do cliente;

- d) Análise do histórico de declarações do Imposto de Renda;
- e) Análise de possíveis protestos;
- f) Análise do histórico de trabalho do cliente, bem como a sua remuneração estimada;
- g) Verificação de recebimento de benefício ou auxílio social governamental;
- h) Verificação da existência de processos judiciais em nome do cliente que possam ser impeditivos de realização do negócio;
- i) Verificação da declaração de que não é Pessoa Exposta Politicamente;
- j) Consulta nas listas impeditivas nacionais e internacionais, como: CNJ, COAF, FBI e ONU;
- k) Consulta nos Sites: Receita Federal, Portal da Transparência, Órgãos Reguladores, SCPC/Serasa, Tribunais Estaduais, Eleitorais, Trabalhistas, Superiores e Mídias;
- l) Análise do relatório de faturamento dos 12 (doze) últimos meses, assinado e datado pelo contador responsável e dos respectivos sócios.
- m) **Background Check** que retorna informações como: (i) PEP (Pessoas Expostas Politicamente); (ii) Mandado de Prisão Expedido; (iii) Consultas às Listas de Sanções Nacionais e Internacionais:
 - **COAF** – Conselho de Controle de Atividades Financeiras
 - **CEAF** – Centro de Estudos e Aperfeiçoamento Funcional
 - **CNEP** – Cadastro Nacional de Empresas Punidas
 - **MTE** – Ministério do Trabalho
 - **CNJ** – Conselho Nacional de Justiça
 - **TSE** – Tribunal Superior Eleitoral
 - **CEIS** – Cadastro de Empresas Inidôneas e Suspensas
 - **EU** – Lista de sanções da União Européia
 - **FBI** – Polícia Federal dos Estados Unidos
 - **GOV UK** – Lista de sanções do Reino Unido
 - **INTERPOL** – Organização Internacional de Polícia Criminal

- **OFAC** – Agência de Controle de Ativos Estrangeiros dos EUA
- **UNSC** – Conselho de Segurança das Nações Unidas
- **Consulta nos Sites:** Receita Federal, Portal da Transparência, Órgãos reguladores, SCPC/Serasa, Tribunais Estaduais, Eleitorais, Trabalhistas, Superiores e Mídias;

n) Verificação de existência de ações judiciais e administrativas.

4.16. Cada candidato a Cliente será verificado antes da aprovação, com base no preenchimento do Formulário de Identificação e verificação da veracidade das informações através do fornecedor homologado e contratado pela **DALPAY**.

4.17. Uma vez adquiridas tais informações, a área responsável envia os documentos e demais informações coletadas para o escritório externo de advocacia, responsável pelo seu processamento para fins de realização do procedimento de Parecer Opinativo acerca do “Know Your Client” da **DALPAY**, dispondo acerca de sua aprovação ou reprovação a ser auferida com base em uma pesquisa realizada em plataformas de busca especializadas, destinadas à verificação de integridade dos indivíduos consultados.

4.18. A verificação da veracidade das informações prestadas pelo responsável do Compliance ao escritório externo de advocacia, são verificadas a partir do sistema do seguinte fornecedor homologado:

- **COMBATE A FRAUDE S.A.** – CNPJ: 34.102.645/0001-57. R. Tiradentes, 1077 - 5º andar – Centro - Venâncio Aires - RS, 95800-000,, site: www.caf.io/pt.

4.19. Os Pareceres Opinativos elaborados pelo escritório de advocacia externo sempre consignarão, em suas conclusões, as ponderações acerca do cliente e das informações consultadas, apontando, assim, por sua aprovação ou reprovação. O referido documento será enviado ao único sócio e administrador da **DALPAY**, o Sr. **DAVIDSON DE ALENCAR LEITE**, que será o responsável final pela decisão acerca do fornecimento dos serviços pela **DALPAY**.

4.19.1. O escritório de advocacia externo elabora apenas pareceres opinativos, de forma que a responsabilidade de seguir ou não com as recomendações expostas são exclusivas dos sócios da empresa. **O ESCRITÓRIO DE ADVOCACIA EXTERNO E A ADVOGADA EXTERNA NÃO POSSUEM, EM NENHUMA HIPÓTESE, CONDÃO DECISÓRIO.**

4.20. O monitoramento das informações e documentos coletados dos Clientes para fins de análise de compliance é realizado a cada 90 (noventa) dias, sendo necessário o reenvio da documentação obrigatória.

4.21. Quanto mais precisas e atualizadas forem as informações coletadas e registradas, maior será a capacidade de identificação de atividades ilícitas.

FLUXO OPERACIONAL



4.22. Após a verificação no sistema, o cliente poderá ser aprovado, com estabelecimento de limites operacionais e sujeito a monitoramento rigoroso de todas as transações, que são enviadas mensalmente à Receita Federal do Brasil.

4.23. Caso o cliente seja reprovado durante o processo de verificação, seu cadastro

será automaticamente bloqueado na Plataforma da **DALPAY**.

4.24. Não é permitido cadastrar-se em nome de terceiros. Em caso de comprovante de endereço em nome de outra pessoa, será necessário verificar o parentesco ou apresentar contrato de locação ou documento similar para comprovação de residência.

4.25. É proibido o cadastro de menores de 18 (dezoito) anos ou incapazes.

4.26. A **DALPAY** reserva-se o direito de não atender ou aceitar Pessoas Expostas Politicamente ("PEP").

4.27. A **DALPAY** não estabelece parcerias nem mantém relações comerciais com países listados em sanções nacionais, nem com clientes que estejam na lista de sanções nacionais e internacionais.

5. PROCEDIMENTOS INTERNOS ADOTADOS PELA EMPRESA

5.1. A **DALPAY** utiliza como referência e analogia a CIRCULAR Nº 3.978, DE 23 DE JANEIRO DE 2020, do Banco Central do Brasil, para seus procedimentos internos com o objetivo de prevenção à lavagem de dinheiro e ocultação de bens, direitos e valores.

5.2. Essa política de prevenção será adotada em todos os setores da empresa, iniciando com a avaliação de seus funcionários, parceiros e prestadores de serviços terceirizados, estendendo-se às operações, transações, produtos, serviços e clientes da **DALPAY**.

5.3. Os presentes procedimentos e esta política serão divulgados aos funcionários da instituição, parceiros e prestadores de serviços terceirizados, em linguagem clara e acessível, com detalhamento compatível com as funções desempenhadas e a sensibilidade das informações.

5.4. A **DALPAY** possui um setor interno de compliance, responsável pela implementação e cumprimento dos procedimentos alinhados e dispostos por

analogia à CIRCULAR Nº 3.978, DE 23 DE JANEIRO DE 2020, do Banco Central do Brasil, conforme estabelecido nesta política.

5.5. Em conformidade com a circular, a **DALPAY** deve implementar uma estrutura de gerenciamento dos riscos operacionais, além de identificar e mensurar o risco de utilização de seus produtos e serviços na prática da lavagem de dinheiro e do financiamento do terrorismo.

5.6. A avaliação interna de risco deverá ser documentada e aprovada pelo diretor, Sr. **DAVIDSON DE ALENCAR LEITE**, e encaminhada aos setores envolvidos em decisões que possam envolver riscos regulatórios e de prevenção à lavagem de dinheiro. É responsabilidade do diretor identificar potenciais riscos, definir métricas e tratar eventuais incidentes identificados.

5.7. Seguindo os procedimentos instituídos pela CIRCULAR Nº 3.978, DE 23 DE JANEIRO DE 2020, do Banco Central do Brasil, adotados pela **DALPAY** por analogia, a empresa deve adotar procedimentos de identificação que permitam verificar e validar a identidade do cliente, obtendo, verificando e validando a autenticidade das informações de identificação do cliente, inclusive, se necessário, mediante confronto dessas informações com dados disponíveis em bancos de dados públicos e privados.

5.8. O Departamento de Compliance da **DALPAY** é exercido por canal direto na própria empresa, tendo como responsável o Sr. **DAVIDSON DE ALENCAR LEITE**, sócio administrador da **DALPAY**. Além disso, a **DALPAY** contrata um escritório de advocacia externo para a elaboração de pareceres opinativos sobre aprovação e reprovação dos Clientes, com a utilização dos seguintes fornecedores homologados:

- **COMBATEAFRAUDE S.A.** – CNPJ: 34.102.645/0001- 57. R. Tiradentes, 1077 - 5º andar – Centro - Venâncio Aires - RS, 95800-000, site: [CAF | Especialistas em validação de identidades e onboarding de clientes](#);

5.9. Adicionalmente, a **DALPAY** utiliza internamente o seguinte fornecedor homologado para a verificação dos Usuários:

- **NETRIN CONSULTORIA E SERVIÇOS EM TECNOLOGIA DA INFORMAÇÃO LTDA.** – CNPJ n.º 13.384.727/0001-61, com sede na Av. Theodomiro Porto da Fonseca, nº 3101, Edifício 08, Sala E, Duque de Caxias, São Leopoldo – RS, CEP: 93.020-080, site: www.netrin.com.br .

5.10. Conforme os procedimentos instituídos pela CIRCULAR Nº 3.978, DE 23 DE JANEIRO DE 2020, do Banco Central do Brasil, adotados pela **DALPAY** por analogia, a empresa deverá adotar procedimentos de qualificação de risco por meio da coleta, verificação e validação de informações compatíveis com o perfil de risco do cliente e a natureza da relação de negócio.

5.11. Os procedimentos estabelecidos pela **DALPAY** para a identificação do cliente e sua qualificação de risco serão detalhados na sequência desta política.

6. GERENCIAMENTO DE RISCO

6.1. Conforme definido na Circular BCB nº 3.681/13, as Instituições de Pagamento devem implementar estrutura de gerenciamento dos riscos operacional, de liquidez e de crédito, entretanto a **DALPAY** não atua como Instituição de Pagamento, mas observa a presente Circular.

6.2. Esta Política de Gerenciamento de Riscos poderá se desdobrar em: **(i)** outras políticas e estratégias aprovadas e revisadas, anualmente, pela diretoria e/ou pela Alta Administração; **(ii)** a criação de documentação acerca das políticas, estratégias de gerenciamento de riscos e governança da **DALPAY**, bem como diretrizes sobre a terceirização de serviços e critérios de seleção de prestadores de serviços; **(iii)** manutenção de documentação acerca das políticas, estratégias de gerenciamento de riscos e governança à disposição do Banco Central do Brasil, com diretrizes sobre a terceirização de serviços e de seleção de seus prestadores, incluindo as condições contratuais mínimas necessárias para mitigar o risco operacional, e a continuidade dos serviços de pagamento prestados.

I - Estrutura de gerenciamento de riscos

a) 1ª linha de defesa: Áreas de Negócios e Suporte.

- A primeira linha de defesa é responsável por monitorar e mitigar os riscos associados às funções e atividades de negócios.

b) 2ª linha de defesa: Riscos, Controles Internos e Compliance.

- A segunda linha de defesa é responsável pela definição de métodos para identificação, avaliação e monitoramento do grau de exposição aos riscos, alinhadas ao apetite de risco da **DALPAY**.

c) 3ª linha de defesa: Auditoria interna

- A terceira linha de defesa é responsável por verificar e realizar avaliação independente e periódica da efetividade das políticas, métodos e procedimentos para controle e gestão dos riscos, além de verificar a sua efetiva implementação.

II - Risco Operacional

6.3. O risco operacional é a ocorrência de perdas resultantes dos seguintes eventos:

- a)** Falhas na proteção e na segurança de dados sensíveis relacionados tanto às credenciais dos usuários finais quanto a outras informações trocadas com o objetivo de efetuar transações de pagamento;
- b)** Falhas na identificação e autenticação do usuário final;
- c)** Falhas na autorização das transações de pagamento;
- d)** Fraudes internas;

- e) Fraudes externas;
- f) Demandas trabalhistas e segurança deficiente do local de trabalho;
- g) Práticas inadequadas relativas a usuários finais, produtos e serviços de pagamento;
- h) Danos a ativos físicos próprios ou em uso pela instituição;
- i) Ocorrências que acarretem a interrupção das atividades da instituição de pagamento ou a descontinuidade dos serviços de pagamento prestados;
- j) Falhas em sistemas de tecnologia da informação; e
- k) Falhas na execução, cumprimento de prazos e gerenciamento das atividades envolvidas em arranjos de pagamento.

6.4. Para prevenção, identificação, mitigação e tratamento de riscos operacionais, a **DALPAY** adotará as seguintes medidas e diretrizes:

- a) Elaboração e implementação de um plano de contingência e outros mecanismos que garantam a continuidade dos serviços de pagamento prestados;
- b) Mecanismos de proteção e segurança dos dados armazenados, processados ou transmitidos;
- c) Mecanismos de proteção e segurança de redes, sítios eletrônicos, servidores e canais de comunicação com vistas a reduzir a vulnerabilidade a ataques;
- d) Procedimentos para monitorar, rastrear e restringir acesso a dados sensíveis, redes, sistemas, bases de dados e módulos de segurança;]

- e) Monitoramento das falhas na segurança dos dados e das reclamações dos usuários finais a esse respeito;
- f) Revisão das medidas de segurança e de sigilo de dados, especialmente depois da ocorrência de falhas e previamente a alterações na infraestrutura ou nos procedimentos;
- g) Elaboração de relatórios que indiquem procedimentos para correção de falhas identificadas;
- h) Realização de testes que assegurem a robustez e a efetividade das medidas de segurança de dados adotadas;
- i) Segregação de funções nos ambientes de tecnologia da informação destinados ao desenvolvimento, teste e produção;
- j) Identificação adequada do usuário final;
- k) Mecanismos de autenticação dos usuários finais e de autorização das transações de pagamento;
- l) Processos para assegurar que todas as transações de pagamento possam ser adequadamente rastreadas;
- m) Avaliações e filtros específicos para identificar transações consideradas de alto risco;
- n) Notificação ao usuário final acerca de eventual não execução de uma transação;
- o) Mecanismos que permitam ao usuário final verificar se a transação foi executada corretamente; e
- p) Documentação e armazenamento de informações relacionadas a perdas

associadas a riscooperacional.

6.5. Caso a **DALPAY** terceirize quaisquer funções relacionadas à segurança na prestação dos seus serviços oferecidos aos Usuários, o contrato de prestação de serviços com estes terceiros deverá prever o disposto nesta Política.

III - Tratamento de Riscos

6.6. Após classificados, os riscos serão analisados para determinar o tratamento adequado. O Tratamento de riscos pela **DALPAY** será desenvolvido através de procedimento a ser criado pela Área de Compliance, a ser definido conforme cada caso, segundo a seguinte definição:

a) RISCOS SOLUCIONÁVEIS: Os riscos solucionáveis são aqueles que a **DALPAY** entende serem passíveis de resolução sem impactos relevantes à operação da **DALPAY**, e assim, conseqüentemente deixarão de ser riscos na medida em que for implementada a resolução;

b) RISCOS MITIGÁVEIS: Os riscos mitigáveis para a **DALPAY** são aqueles para os quais, há ações paramitigação e que assim, continuam a existir só que com menor gravidade. c. são aqueles que sefaz a assunção do risco, ou seja, que a **DALPAY** aceita correr sem estabelecer medidas de mitigação, visto que entende que o risco seria baixo ao seu negócio.

IV - Procedimento de Correção de Falhas

6.7. Os procedimentos de correção de falhas deverão abordar:

a) Identificação de Perdas Operacionais: a apuração da perda decorrente de Incidente constitui fator importante para o cumprimento das exigências dos órgãos reguladores além de prover a **DALPAY** informações consistentes, padronizadas e atualizadas, decisivas para uma análise quantitativa do gerenciamento do risco na **DALPAY**;

b) Avaliação da Qualidade dos Controles: a avaliação dos controles tem como

objetivo avaliar a efetividade/eficiência dos controles, a fim de verificar se estes estão sendo executados conforme descritos nas matrizes de risco e políticas internas;

c) Plano de Treinamento: o plano de treinamento tem como objetivo, por meio de simulações de incidentes e avaliação de incidentes ocorridos, garantir que os Colaboradores estejam preparados para lidar com incidentes e aptos a identificar situações de riscos e vulnerabilidades.

7. CRITÉRIOS DE APROVAÇÃO

7.1 Após a obtenção dos resultados das buscas feitas pela **DALPAY** no software provido por seu fornecedor homologado, o escritório externo de advocacia contratado pela **DALPAY** realiza uma análise pormenorizada a respeito dos resultados, a fim de interpretar as informações obtidas para assim opinar acerca da possibilidade ou não de prestação de serviços para o cliente.

7.2 O ESCRITÓRIO DE ADVOCACIA EXTERNO NÃO POSSUI, EM NENHUMA HIPÓTESE, CONDÃO DECISÓRIO.

7.3 Ao longo de sua análise, o responsável pelo compliance da **DALPAY** irá utilizar-se dos seguintes critérios analíticos:

- a) Existência de protestos;
- b) Histórico de declarações de imposto de renda;
- c) Histórico de vínculos empregatícios contemporâneos e passados;
- d) Cadastro em conselhos de profissão;
- e) Renda própria estimada;
- f) Patrimônio estimado;

- g)** Usufruto de programas governamentais de assistência social;
- h)** Inscrição do cliente em listas restritivas de qualquer natureza;
- i)** Cadastro do cliente em quaisquer autarquias ou associações controladoras;
- j)** Existência de ficha atribuível ao cliente em qualquer agência nacional ou internacional anticrimes;
- k)** Existência de processos judiciais de qualquer natureza;
- l)** Natureza dos processos judiciais eventualmente existentes;
- m)** Qualidade de Pessoa Exposta Politicamente (“PEP”).

7.4 Muito embora a lista de critérios seja extensa, é importante ressaltar que a conclusão final a ser tomada pelo responsável pelo Compliance acerca da aprovação ou não do cliente em muito dependerá da natureza dos apontamentos levantados pelo software de busca, e não por sua quantidade total.

7.5 De todo modo, serão critérios definitivos na reprovação do cliente:

- a)** A existência de processos judiciais de natureza criminal de qualquer tipo;
- b)** Envolvimento em escândalos de natureza fiscal, econômica ou pública;
- c)** Sua inscrição em cadastros protetivos de crédito;
- d)** Sua inscrição em lista restritiva;
- e)** Passagem por qualquer autoridade policial, seja ela nacional ou internacional.

f) A falta de lastro financeiro que comprove o poderio monetário para a realização da operação desejada.

7.6 Em resumo, o processo de verificação e análise de clientes pela **DALPAY** é rigoroso e detalhado, visando garantir a segurança e a conformidade com as normas legais e regulatórias. Através da utilização de tecnologia avançada e da análise criteriosa conduzida por profissionais especializados, a **DALPAY** assegura que apenas clientes qualificados e com histórico adequado possam utilizar seus serviços, protegendo assim a integridade da empresa e de seu ecossistema financeiro.

8. LIMITES OPERACIONAIS

8.1 Os limites operacionais foram desenhados de forma a serem condizentes com a capacidade econômico-financeira, combinando com a utilização de Abordagem Baseada em Risco (“ABR”), onde mensura-se a exposição aos riscos a partir dos dados pessoais do cliente.

8.2 A **DALPAY** possui limites operacionais amparados da seguinte forma:

I – OPERAÇÕES ATRAVÉS DE CORRETORAS EXTERNAS

a) Classificação Nível 1 – Até R\$ 10.000,00

- **Depósito: Reais:** R\$ 10.000,00
- **Stablecoins:** R\$ 10.000,00
- **Limite Semanal**
- **Saque-Reais:** R\$ 10.000,00
- **Bitcoin:** 2 BTC

Solicitação Nível 1:

- Verificação padrão realizada pela corretora escolhida.

b) Classificação Nível 2 – De R\$ 10.000,001 a R\$ 49.999,99

- **Depósito: Reais:** R\$ 49.999,99
- **Stablecoins:** R\$ 49.999,99
- **Limite Semanal**
- **Saque-Reais:** R\$ 49.999,99
- **Bitcoin:** 4 BTC

Solicitação Nível 2:

- Verificação adicional do CPF ou CNPJ - Background Check básico das seguintes informações: **i)** PEP (Pessoas Expostas Politicamente); **ii)** Ações judiciais criminais; **iii)** Patrimônio declarado; **iv)** Histórico financeiro.

c) Classificação Nível 3 – A partir de R\$ 50.000,00

- **Depósito: Reais:** R\$ 50.000,00 ou mais
- **Stablecoins:** R\$ 50.000,00 ou mais
- **Limite Semanal**
- **Saque-Reais:** R\$ 50.000,00 ou mais
- **Bitcoin:** 8 BTC ou mais

Solicitação Nível 3

- Verificação adicional do CPF ou CNPJ - Background Check das seguintes informações: **i)** PEP (Pessoas Expostas Politicamente); **ii)** Ações judiciais criminais; **iii)** Patrimônio declarado; **iv)** Histórico financeiro; **v)** Lista de Sanções Nacionais e Internacionais como:

- COAF – Conselho de Controle de Atividades Financeiras
- CEAF – Centro de Estudos e Aperfeiçoamento Funcional
- CNEP – Cadastro Nacional de Empresas Punidas
- MTE- Ministério do Trabalho

- CNJ – Conselho Nacional de Justiça
- TSE – Tribunal Superior Eleitoral
- CEIS – Cadastro de Empresas Inidôneas e Suspensas
- EU – Lista de sanções da União Européia
- FBI – Polícia Federal dos Estados Unidos
- GOV UK – Lista de sanções do Reino Unido
- INTERPOL – Organização Internacional de Polícia Criminal
- OFAC – Agência de Controle de Ativos Estrangeiros dos EUA
- UNSC- Conselho de Segurança das Nações Unidas
- Consulta nos Sites: Receita Federal, Portal da Transparência, Órgãos reguladores, SCPC/Serasa, Tribunais

II – OPERAÇÕES NA PLATAFORMA DALPAY

d) Classificação Nível 1 – Até R\$ 10.000,00

- **Depósito: Reais:** Até R\$ 10.000,00
- **Stablecoins:** Até R\$ 10.000,00
- **Limite Semanal**
- **Saque-Reais:** Até R\$ 10.000,00
- **Bitcoin:** 2 BTC

Solicitação Nível 1 (a partir da 2ª operação):

- Submissão de documento de identificação pessoal válido e autêntico;
- Submissão de prova de vida, que consiste em envio de Selfie (foto de si mesmo) segurando o documento de identificação pessoal;
- Submissão de comprovante de residência de até 03 (três) meses anteriores;
- Background Check básico das seguintes informações: **i)** PEP (Pessoas Expostas Politicamente); **ii)** Mandado de Prisão Expedido; **iii)** Listas de Sanções Nacionais e Internacionais (CEPIM, CEIS, CNEP, UNSC, COAF, OFAC, INTERPOL); **iv)** Ações judiciais e administrativas.
- Declaração de wallets do usuário;

- Recibo das Declarações de IN 1888/2019.

e) Classificação Nível 2 – De R\$ 10.000,01 a R\$ 49.999,99

- **Depósito: Reais:** R\$ 10.000,001 a R\$ 49.999,99
- **Stablecoins:** R\$ 10.000,001 a R\$ 49.999,99
- **Limite Semanal**
- **Saque-Reais:** R\$ 10.000,001 a R\$ 49.999,99
- **Bitcoin:** 4 BTC

Solicitação Nível 2:

- Submissão de documento de identificação pessoal válido e autêntico;
- Submissão de prova de vida, que consiste em envio de Selfie (foto de si mesmo) segurando o documento de identificação pessoal;
- Submissão de comprovante de residência de até 3 (três) meses anteriores;
- Background Check que retorna informações como: **i)** PEP (Pessoas Expostas Politicamente); **ii)** Mandado de Prisão Expedido; **iii)** Listas de Sanções Nacionais e Internacionais (CEPIM, CEIS, CNEP, UNSC, COAF, OFAC, INTERPOL); **iv)** Ações judiciais e administrativas.
- Declaração de wallets do usuário;
- Recibo das Declarações de IN 1888/2019.

f) Classificação Nível 3 – A partir de R\$ 50.000,00

- **Depósito: Reais:** R\$ 50.000,00 ou mais
- **Stablecoins:** R\$ 50.000,00 ou mais
- **Limite Semanal**
- **Saque-Reais:** R\$ 50.000,00 ou mais
- **Bitcoin:** 8 BTC ou mais

Solicitação Nível 3

- Submissão de documento de identificação pessoal válido e autêntico;
- Submissão de prova de vida, que consiste em envio de Selfie (foto de si

mesmo) segurando o documento de identificação pessoal;

- Submissão de comprovante de residência de até 03 (três) meses anteriores;
- Background Check que retorna informações como: **i)** PEP (Pessoas Expostas Politicamente); **ii)** Mandado de Prisão Expedido; **iii)** Listas de Sanções Nacionais e Internacionais (CEPIM, CEIS, CNEP, UNSC, COAF, OFAC, INTERPOL); **iv)** Ações judiciais e administrativas;
- Busca de Mídia Negativa;
- Submissão de formulário de Onboarding para fins de declaração e comprovação de capacidade econômico-financeira, com a devida demonstração da origem dos recursos a serem investidos;
- Submissão de documentos e constitutivos (PJ): **i)** Cópia do Contrato Social; **ii)** Cópia do Documento de Identificação do QSA; **iii)** Comprovante de endereço da empresa;
- Submissão de documentos financeiros: **i)** extrato bancário; **ii)** Balanço contábil assinado por contador; **iii)** Cópia da primeira página da Declaração de Imposto de Renda; **iv)** Documento comprobatório do faturamento médio mensal dos últimos doze meses; **v)** Outro documento hábil a demonstrar a situação financeira patrimonial e lastro financeiro para as operações; **vi)** Demonstração de lastro financeiro de capital mensal de R\$ 500.000,00 (quinhentos mil reais); **vii)** Recibo das Declarações de IN 1888/2019.

9. ABORDAGEM BASEADA EM RISCO

9.1. Em compasso com as recomendações do GAFI/FATF e demais normas de referência, a Política se perfaz em especial através do procedimento de Abordagem de Risco (identificação de fatores de determinação do risco), a fim e detectar as suspeitas nas operações e reportá-las.

9.2. Os riscos são subdivididos em:

ALTO (REPROVADOS)	I) Clientes domiciliados ou sediados em cidades de fronteira com outros países;
Os riscos são significativos, normalmente reprovados no	

Onboarding. A **DALPAY** deve aplicar controles mais restritivos para reduzir o risco, tais como diligência reforçada e o monitoramento mais rigoroso.

- II) Clientes que sejam Pessoa Politicamente Exposta (“PPE”);
- III) Clientes que declarem ter pelo menos uma das atividades abaixo:

- a) Sem atividade formal;
- b) Comercialização de joias, pedras e metais preciosos, objetos de arte e antiguidades;
- c) Compra e venda de imóveis;
- d) Revenda de automóveis usados;
- e) Comércio de armamento;
- f) Empresas de turismo;
- g) Importação e Exportação;
- h) Clubes esportivos;
- i) Igrejas e congregações religiosas;
- j) Casas de apostas, cassinos ou jogos de azar.

MÉDIO

Os riscos precisam de análise adicional e a decisão deve ser tomada pela **DALPAY**.

- I) Empresas sem comprovação de lastro suficiente para garantir as operações;
- II) Empresas com ações judiciais não impeditivas da atividade;
- III) Empresas cujos sócios não possuem histórico com movimentação em criptoativos.

BAIXO

Representa o Risco Base em relação ao qual as regras comerciais normais são aplicáveis.

- I) Clientes que tenham comprovado renda e a origem dos valores;
- II) Clientes com o código de atividade econômica correto;
- III) Clientes que enviaram os Recibos exigidos pela IN 1888/2019 da RFB.
- IV) Clientes que enviaram a documentação de identificação

completa e não possuem ações judiciais.

9.3. Cada cliente e parceiro da **DALPAY** recebe uma designação de risco de acordo com o seu perfil, o que orienta, em grande parte, as diligências a serem aplicadas de maneira específica. O tratamento baseado no equilíbrio de riscos assegura que os casos com maior impacto negativo sejam tratados de forma diferenciada. Essa abordagem personalizada permite ajustar as medidas de due diligence e monitoramento conforme a avaliação de risco associada a cada cliente e parceiro, garantindo uma resposta proporcional às características específicas de cada caso.

9.4. Para garantir a segurança e proteção das contas dos usuários, a **DALPAY** está comprometida em cumprir os regulamentos de Prevenção à Lavagem de Dinheiro (AML) e Combate ao Financiamento do Terrorismo (CTF). Em nossos esforços contínuos para cumprir obrigações regulatórias, poderemos precisar coletar informações adicionais e documentos de apoio relacionados à Fonte dos Recursos (SOF) e à Fonte de Renda e Patrimônio (SOW) dos usuários em determinados casos. Documentos de Fonte dos Recursos aceitáveis:

ANÁLISE KYT	DOCUMENTOS COMPROBATÓRIOS
Salário	<ul style="list-style-type: none"> - Folhas de pagamento mostrando a renda pelo menos do último mês; - Extrato bancário comprobatório dos pagamentos de salário pela entidade patronal, pelo menos, do último mês; - Declaração de impostos do ano fiscal anterior.
Autônomo	<ul style="list-style-type: none"> - Declaração de impostos do ano fiscal anterior; - As últimas faturas/contratos/convênios de prestação de serviços autônomos ou demonstrativo de lucros/perdas, comprovando sua renda mensal ou anual.

Auxílio/Subsídio	<ul style="list-style-type: none"> - Extrato bancário das transferências de mesadas dos últimos 3 meses; - Subsídio emitido pelo governo ou outro extrato de benefícios sociais.
Economias Pessoais	<ul style="list-style-type: none"> - Extratos de contas bancárias de poupança emitido nos últimos 3 meses; - Declaração de IRPF com detalhamento de bens e direitos; - Declaração de saldo bancário emitida pelo banco.
Pensão	<ul style="list-style-type: none"> - Extrato bancário comprovando as transferências de pensões dos últimos 3 meses; - Declaração de pensão emitida pelo governo; - Demonstrativos do fundo de pensão.
Pagamentos de dividendos/lucro de uma empresa	<ul style="list-style-type: none"> - Declaração de dividendos; - Contratos de Distribuição; - Extrato bancário mostrando pagamentos de dividendos; - Últimas contas auditadas da empresa.
Leaseback	<ul style="list-style-type: none"> - Contrato de leaseback; - Extratos bancários demonstrando os recebimentos; - Documentação contábil que detalhe a transação.
Dia de Comércio	<ul style="list-style-type: none"> - Extratos de transações comprovando a atividade de trading do último mês; e - Extrato bancário mostrando saques de lucros de trading depositados na conta. *Ambos os documentos devem mostrar os detalhes de registro da conta e o logotipo do emissor. - Declaração de rendimentos do ano fiscal anterior, comprovando os rendimentos do exercício.
Jogos de azar	<ul style="list-style-type: none"> - Extratos de transações comprovando a atividade de jogo no último mês; e - Extrato bancário mostrando as retiradas de lucros de jogos de azar depositados na conta. *Ambos os documentos devem mostrar os detalhes de registro da conta e o logotipo do emissor.

	<ul style="list-style-type: none"> - Declaração de rendimentos do exercício anterior, comprovando os rendimentos de jogos de azar.
Renda Passiva	<ul style="list-style-type: none"> - Um contrato de aluguel/empréstimo assinado E um dos seguintes: <ul style="list-style-type: none"> a. Extrato bancário, mostrando o último pagamento de aluguel/empréstimo; b. Últimos recibos de aluguel/empréstimo; - Quaisquer outros documentos que comprovem sua renda passiva (por exemplo, royalties de livros, marketing de afiliados, staking, etc.) no último mês.
Empréstimos/Hipotecas	<ul style="list-style-type: none"> - Um contrato de empréstimo/hipoteca mostrando o valor do empréstimo e o plano de amortização; e um extrato bancário mostrando um depósito de empréstimo/hipoteca em sua conta.
Debênture	<ul style="list-style-type: none"> - Certificado de debênture; - Extratos de corretoras ou bancos confirmando a propriedade das debêntures; - Declaração de IRPF com a inclusão das debêntures.
Venda de Ativos Financeiros	<ul style="list-style-type: none"> - Declaração do provedor de investimentos; - Extrato bancário exibindo liquidação do provedor de investimento; - Outras declarações ou documentos que comprovem o lucro do investimento (de títulos, ações, etc.).
Venda de Imóveis ou Outros Ativos	<ul style="list-style-type: none"> - Contrato de venda/declaração de liquidação; - Carta assinada de um administrador/advogado/agente imobiliário confirmando a venda do imóvel; - Cópias do registro de imóvel/título de propriedade. *Também aceitamos o extrato bancário mostrando o depósito dos fundos da venda em sua conta bancária.
Herança	<ul style="list-style-type: none"> - Cópia do testamento/inventário; - Carta assinada do testamenteiro/ advogado/ administrador/ concessão do inventário.
Doações	<ul style="list-style-type: none"> - Contrato de doação para imóveis ou outros bens; - Declaração/carta assinada do doador declarando a natureza do presente;

	- Extrato bancário comprovando o depósito bancário da doação.
Indenização de Ações Judiciais	- Sentença judicial ou acordo judicial; - Comprovantes de pagamento recebidos; - Extratos bancários demonstrando os depósitos.
Mineração de Criptomoedas	- Comprovante de compra do hardware usado para mineração (mostrando seus dados e o endereço do vendedor); - Comprovante de todas as receitas de mineração da(s) plataforma(s)/corretora(s) relevante(s). *Forneça capturas de tela do seu histórico de transações (por pelo menos 3 meses), detalhando todas as atividades com as moedas extraídas e exibindo endereços de carteira e IDs de transação. Estes devem ser capturados da plataforma/corretora correspondente e devem incluir os detalhes da sua conta.

10. MECANISMOS E MÉTRICAS DE AVALIAÇÃO DE RISCO

10.1. Os mecanismos e métricas de avaliação de risco foram desenvolvidos em alinhamento com as especificidades do modelo de negócio da **DALPAY** e seu porte. Essa mensuração ocorre através da criação de matrizes que apresentam ponderações sobre os fatores de risco, conferindo uma estrutura para a análise sistemática dos riscos envolvidos nas operações da empresa, e são projetadas para considerar vários aspectos, como:

a) Persecução penal:

- Terrorismo, inclusive financiamento do terrorismo;
- Tráfico de seres humanos e contrabando de migrantes;
- Exploração sexual, inclusive de crianças;
- Lavagem de dinheiro;
- Participação em grupo criminoso organizado e crime organizado;
- Tráfico de narcóticos e substâncias psicotrópicas;
- Tráfico de armas;

- Corrupção e suborno;
- Fraude;
- Improbidade administrativa;
- Crimes contra o SFN (Lei 7.492/86);
- Falsificação de moeda;
- Falsificação e pirataria de produtos;
- Crimes ambientais;
- Lobismo (atos de pressão sobre pessoas ou poderes públicos);
- Homicídio, lesão corporal grave;
- Sequestro, privação ilegal de liberdade e tomada de reféns;
- Roubo ou furto;
- Contrabando;
- Crimes fiscais (relacionados a impostos diretos e indiretos);
- Extorsão;
- Falsificação;
- Pirataria; e
- Utilização de informação privilegiada e manipulação do mercado;

b) PEP ou PPE (Pessoa Exposta Politicamente): É dada uma especial atenção quanto às operações realizadas pelas pessoas que se enquadrem nesta categoria e àqueles que possuem relacionamento próximo com PEPs, uma vez que são agentes que estão mais expostos à prática de atos ilícitos e oferecem maior risco ao Sistema Financeiro Nacional. A **DALPAY** se reserva ao direito de não aprovar PEP. São consideradas politicamente expostas aquelas pessoas que desempenham ou tenham desempenhado, nos últimos 05 (cinco) anos, cargos, empregos ou funções públicas relevantes, no Brasil ou em outros países, territórios e dependências estrangeiros, assim como seus representantes, familiares e outras pessoas de seu relacionamento próximo.

c) Domicílio em País não cooperante (Specially Designated Nations);

d) Sanções em listas restritivas;

e) Localização Geográfica;

f) Mídia negativa.

10.2. Para concluir, os mecanismos e métricas de avaliação de risco estabelecidos pela **DALPAY** refletem seu compromisso em garantir a conformidade e a segurança nas operações. Por meio de uma análise abrangente que aborda diversos aspectos, desde a persecução penal até a mídia negativa, a empresa busca mitigar os riscos associados a atividades ilícitas. Esses esforços demonstram a dedicação da **DALPAY** em manter um ambiente operacional seguro e em conformidade com as regulamentações vigentes, protegendo assim seus clientes e parceiros.

11. PESSOAS EXPOSTAS POLITICAMENTE (PEP)

11.1. A **DALPAY** dedica especial atenção durante os procedimentos de cadastro, contratação, atualização de informações, prestação de serviços e monitoramento de operações de clientes e colaboradores. A empresa adota rigorosos critérios de conformidade para assegurar que não opera, atende ou contrata Pessoas Expostas Politicamente (PEP). Este cuidado é essencial para mitigar riscos e garantir a integridade das operações, conforme estabelecido nas diretrizes de compliance e regulamentações aplicáveis. A **DALPAY** mantém um controle contínuo e atualizado para identificar e excluir quaisquer PEPs de suas atividades, preservando assim a segurança e a confiabilidade de seus serviços.

12. PROTEÇÃO DE DADOS PESSOAIS

12.1. A coleta, acesso e tratamento de dados pessoais de Clientes, colaboradores e fornecedores pessoas físicas pela **DALPAY** são necessários para cumprir as obrigações desta Política, estando em conformidade com a Lei Geral de Proteção de Dados (Lei nº 13.709, de 14 de agosto de 2018).

12.2. Não obstante, a **DALPAY**, seus colaboradores e fornecedores têm o dever de zelar pela segurança e privacidade dos dados pessoais tratados. A utilização desses dados deve ocorrer dentro dos limites necessários à proposta específica, com

transparência e em conformidade com a legislação vigente, incluindo a Política de Privacidade da **DALPAY**.

13. DIRETORIA DE ÉTICA E COMPLIANCE

13.1. A Diretoria de Ética e Compliance da **DALPAY** é presidida pelo Responsável pelo Departamento de Compliance. É neste fórum que são tomadas as decisões que envolvem riscos regulatórios e medidas de prevenção à lavagem de dinheiro. O Responsável pelo Departamento de Compliance é responsável pela identificação de potenciais riscos, definição de métricas e tratamento dos incidentes identificados.

14. DEPARTAMENTO DE COMPLIANCE

14.1. O Departamento de Compliance da **DALPAY** é exercido por canal direto na própria empresa, tendo como responsável o Sr. **DAVIDSON DE ALENCAR LEITE**, sócio administrador da **DALPAY**. Além disso, a **DALPAY** contrata um escritório de advocacia externo para a elaboração de pareceres opinativos sobre aprovação e reprovação dos Clientes, com a utilização do seguinte fornecedor homologado:

- **COMBATE A FRAUDE S.A.** – CNPJ: 34.102.645/0001- 57. R. Tiradentes, 1077 - 5º andar – Centro - Venâncio Aires - RS, 95800-000, site: www.caf.io/pt.

14.2. Adicionalmente, a **DALPAY** utiliza internamente o seguinte fornecedor homologado para a verificação dos Usuários:

- **NETRIN CONSULTORIA E SERVIÇOS EM TECNOLOGIA DA INFORMAÇÃO LTDA.** – CNPJ n.º 13.384.727/0001-61, com sede na Av. Theodomiro Porto da Fonseca, nº 3101, Edifício 08, Sala E, Duque de Caxias, São Leopoldo – RS, CEP: 93.020-080, site: www.netrin.com.br.

14.3. O Departamento de Compliance atua com as seguintes responsabilidades:

- a) Executar os controles dos processos de KYC e PLD/CFT;

- b)** Identificar e avaliar os riscos de Compliance das gerências proprietárias de riscos;
- c)** Direcionar e treinar os stakeholders, diretoria, gerências e todos os colaboradores em assuntos de Compliance;
- d)** Monitorar continuamente e relatar novos riscos de Compliance identificados nos negócios;
- e)** Elaborar junto às gerências responsáveis por cada área de negócio as políticas e procedimentos que devem estar alinhadas ao Código de Conduta e Ética da **DALPAY**, mitigando os riscos já mapeados;
- f)** Assessorar a Administração e as áreas de negócio nas tomadas de decisão que envolvem riscos.

14.4. A **DALPAY** entende que o Compliance dentro da empresa deve ser independente, com funções que incluem:

- a)** Viabilizar a aderência e cumprimento de leis, regras e normas aplicáveis ao negócio;
- b)** Avaliar a observância de Princípios éticos e Normas de Conduta;
- c)** Implementar e atualizar regulamentos e normas internas;
- d)** Estabelecer Procedimentos e Controles Internos;
- e)** Aplicar testes periódicos e elaborar planos de contingência;
- f)** Avaliar a segregação de funções a fim de evitar conflitos de interesses;
- g)** Avaliar Riscos e Controles Internos, através de relatório (Gestão de Compliance);

h) Desenvolver Políticas Internas que previnam problemas de não conformidade;

i) Fomentar o desenvolvimento da Cultura de: **(i)** prevenção a lavagem de dinheiro através de treinamentos específicos; **(ii)** controle, juntamente com os demais pilares do sistema de controles internos, na busca da conformidade; **(iii)** interlocução com Órgãos Reguladores e Fiscalizadores, Associações de Classe e importantes participantes do mercado; **(iv)** promoção da profissionalização da função e auxílio na criação de mecanismos de revisão de regras de mercado, legislação e regulamentações pertinentes.

15. ATUALIZAÇÃO CADASTRAL

15.1. A **DALPAY** deve identificar alterações substanciais e relevantes nas informações que possui sobre seus clientes, garantindo a adequada alimentação de seus sistemas e a mensuração dos riscos associados aos relacionamentos estabelecidos. É obrigatória a atualização anual dessas informações.

15.2. A precisão dos dados cadastrais é fundamental para o monitoramento eficaz das operações, possibilitando a análise detalhada para identificação de situações que possam indicar lavagem de dinheiro e financiamento ao terrorismo.

16. CANAL DE DENÚNCIAS

16.1. A **DALPAY** conta com um canal de comunicação que permite o recebimento de denúncias no que tange às irregularidades, admitindo-se inclusive denúncias anônimas, sendo proibida a retaliação de denunciante. O canal é destinado tanto ao público interno quanto ao público externo e está disponível na Plataforma **DALPAY**.

16.2. A **DALPAY** garante a confidencialidade e a proteção ao denunciante de boa-fé, valendo-se de um procedimento transparente no que concerne ao acompanhamento da denúncia.

16.3. A denúncia será tratada pelo Departamento de Compliance, que é responsável por tomar os depoimentos das partes envolvidas, examinar a documentação existente, se houver, e realizar o que for necessário para que sejam tomadas providências e penalidades cabíveis a depender da decisão final da Diretoria da **DALPAY**.

16.4. O canal direto da Diretoria Executiva ficará a cargo do Diretor responsável através do e- mail: sac@dalpay.com.br.

17. LEGISLAÇÃO APLICÁVEL E FORO

17.1. A presente Política é regida pela legislação brasileira. Dúvidas e situações não previstas neste instrumento poderão ser encaminhadas aos Canais de Atendimento disponibilizados na Plataforma, e serão primeiramente resolvidas pela **DALPAY**. Caso persistam, deverão ser solucionadas pelos órgãos do sistema brasileiro de defesa do consumidor.

17.2. Quaisquer disputas ou controvérsias oriundas de quaisquer atos praticados no âmbito da utilização das Aplicações pelos Usuários, inclusive com relação ao descumprimento desta Política ou à violação dos Termos de Uso e direitos da **DALPAY**, de seus empreendimentos, de outros Usuários e/ou de terceiros, de direitos de propriedade intelectual, de sigilo e de personalidade, serão processadas no foro da Comarca da Capital do Rio de Janeiro – RJ, considerado o único competente para resolver qualquer controvérsia originada neste instrumento, com expressa renúncia a qualquer outro, por mais privilegiado que seja.

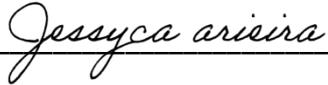
18. APROVAÇÃO E VIGÊNCIA

18.1. Esta Política foi elaborada pela Dra. Jessyca Arieira Araújo - OAB/RJ 201.582, responsável exclusivamente pela elaboração das políticas, e foi aprovada pela Diretoria Executiva da **DALPAY**.

18.2. Este documento tem vigência indeterminada, devendo ser revisado

anualmente ou sempre que necessário.

Rio de Janeiro, 21 de junho de 2024.



Responsável pela Elaboração das Políticas
JESSYCA ARIEIRA ARAÚJO
OAB/RJ 201.582

COO & Representante Legal
DAVIDSON DE ALENCAR LEITE